



TPWD Mobile Application Guidelines

Version: 1.1.final
Revision Date: 7/29/2015

Table of Contents

1.0 OVERVIEW	4
1.1 Purpose	4
1.2 Audience	4
1.3 Prerequisites	4
1.4 Background	4
2.0 CONTENT	4
2.1 Data	5
2.1.1 Data Management Best Practices	5
2.1.2 Public Use	5
2.1.3 Classification of Data	5
2.2 Best Practices.....	5
2.2.1 User Information	5
2.2.2 User Experience	6
2.3 Branding	6
2.3.1 External.....	6
2.3.2 Internal	6
2.4 Security	6
2.4.1 General.....	6
2.4.2 Compliance	6
2.5 Privacy	6
2.6 Accessibility and Usability	7
2.7 Web Services	7
2.8 Revenue and Advertising	7
3.0 MOBILE NATIVE.....	10
3.1 Definition	10
3.2 Architecture.....	10
3.3 Platforms.....	10
3.3.1 IOS Native	10
3.3.2 Android Native.....	11
3.3.3 Multi – Platform Native	11
3.3.4 Other	11
3.4 Authentication and Security	12
3.4.1 OAuth.....	12
3.4.2 Encryption.....	12

4.0	MAINTENANCE AND SUNSET	12
5.0	GLOSSARY.....	12
6.0	REVISION HISTORY.....	12
7.0	APPENDIX	13

1.0 Overview

1.1 Purpose

The purpose of this document is to provide guidelines for the development of mobile applications by Texas Parks and Wildlife and nonprofit partners.

The creation of a mobile application requires following the process outlined in the Mobile Methodology ¹.

For the purposes of this document, mobile applications are defined as software optimized to run on a mobile device. These include native applications running on the device or mobile web applications running on a browser on the mobile device.

Disclaimer: The creation of any application(s) by following these guidelines does not ensure the application be considered an official agency application.

1.2 Audience

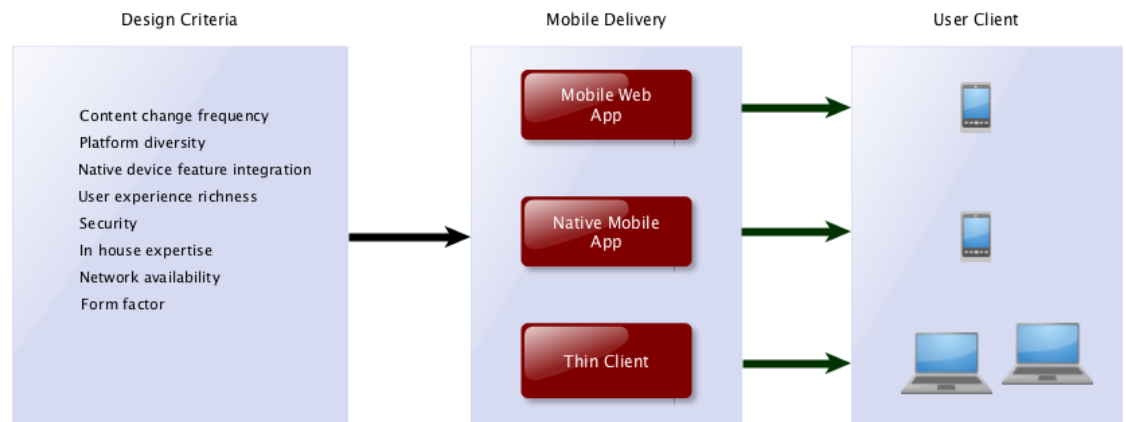
The target audience includes, but is not limited to, internal and external developers, users of agency mobile applications and those requesting mobile application development.

1.3 Prerequisites

The mobile application to be developed must be approved by Governance and follow the Mobile Methodology Guidelines pertaining to the mobile application development process.

1.4 Background

The evolution and proliferation of mobile devices has made mobile technology an essential requirement for government and public end users. The rapidly growing need to produce mobile applications that will enhance the public user experience as well as provide our own internal staff mission critical access to data in remote locations necessitates the creation of a set of guidelines for our agency to develop innovative mobile applications.



2.0 Content

2.1 Data

2.1.1 Data Management Best Practices

The following are current practices in Texas government that support sound data management:

- Texas state agencies are required to develop controls to ensure the confidentiality, integrity, and availability of data.
- Agencies implement internal data governance structures to guide agency-wide data decisions and policies.
- The Texas Legislature recognizes the importance of open data and, through statute, requires state agencies to post high-value data sets in a standard format that allows the public to search, extract, organize, and analyze the information.
- [Texas.gov](https://www.texas.gov) provides a centralized site that offers links to open data posted by state agencies for public use.

2.1.2 Public Use

Public use of data appearing on agency websites is subject to [1 TAC 206](#) covering state websites, as defined by the Department of Information Resources (DIR). Specifically the [State Agency Link and Privacy Policy](#) spells out the policies for linking to, the use of, or copying information from State of Texas agency websites as follows:

- a) Each state agency must publish a linking notice to inform members of the public of the state's policy, and state agency's policy, that govern the use of, copying information from, or linking to a state website.
- b) Each state agency must publish the linking notice on its home page and all key public entry points, or on its site policies page.
- c) The Linking notice:
 - (1) Must be consistent with the State Website Linking and Privacy Policy published on the Department's website.
 - (2) Must include the agency's standards and criteria for linking to a third party website.

2.1.3 Classification of Data

Classification of agency data according to the classification schema noted in the TPWD Security Standards for [Data Classification](#) is the responsibility of the TPWD data stakeholders with assistance from TPWD IT Security and Project Management. The [IT Data Classification form](#) is required to be filled out by the data stakeholder(s) and submitted to the agency ISO for approval.

For more information, please contact TPWD IT Security at TPWD.ITSecurity@tpwd.texas.gov.

2.2 Best Practices

2.2.1 User Information

Each external application should include an end user license agreement, privacy policy (See 2.5), and disclaimer if necessary. These documents should be displayed at the initial start of the application and should be accepted by the user before the application continues.

Documentation must be approved by Legal. See Appendix for boilerplate examples.

2.2.2 User Experience

Acquire Communications division approval during the design process for a consistent user experience. Please contact cis@tpwd.texas.gov.

2.3 Branding

2.3.1 External Apps

Written approval from Communications division is required for all external facing mobile applications wanting to use the TPWD agency brand(s). For more information, please contact Communications Creative and Interactive Services Group at cis@tpwd.texas.gov.

Applications developed not for the agency but for third parties, such as Friends Groups, cannot carry the Texas Parks & Wildlife brand nor can they be designated as an official app of the agency and instead they must use their own logo.

2.3.2 Internal Apps

It is recommended, but not required that non-public facing internal mobile applications follow the same branding requirements as external public facing applications.

2.4 Security

2.4.1 General

Agency security and data classification standards are set forth in the [TPWD IT Security Policy, Standards and Guidelines](#). These policies govern such items as Data classification, information ownership, System Development and acceptable use.

For more information, please contact TPWD IT Security at TPWD.ITSecurity@tpwd.texas.gov.

2.4.2 Compliance

The [TPWD IT Security Policy, Standards and Guidelines](#) are based on TAC 202 requirements to aid in enforcing cyber security of agency data. All applications must be designed within the constraints of the standards and the TPWD SDLC.

2.5 Privacy

The Texas Department of Information Resources [Privacy Policy](#) governs the protection of individual privacy rights in regards to information collected by a state governmental body.

The privacy policy is separate from the TPWD Security Standards and should explicitly state the terms of use of any information gathered from the user of the application. This information may include but is not limited to such items as personal information, device location, and other device data.

Notification to the user in the privacy policy should include the possible use of such data in analytics. In such cases where analytics will rely on anonymous data, this requirement may be waived, but it is still encouraged that the user be notified of the use of collected data in analytics. See data classification for the distinction between anonymous and personable data.

2.6 Accessibility and Usability

Accessibility support for native mobile applications is operation system and device dependent. Please refer to the guidelines provided by each individual vendor for further information.

For official agency applications, external vendors must provide, perform and pass accessibility testing. Approval will be required from the Agency before publication.²

2.7 Web Services

It is highly recommended that web services be used as the standard for exchange of data to and from mobile applications.

A web service is a method of communication between two electronic devices over a network. There are two major classes of web services, REST-compliant web services (stateless), and arbitrary web services that may expose an arbitrary set of operations. WSDL and SOAP are categorized in the arbitrary web services.

For our purposes, we are primarily interested in REST-compliant web services for mobile development due to the nature of intermittent network availability inherent with mobile devices.

REST is short for representational state transfer. Its architectural properties include being stateless, cacheable, and having a uniform interface. Applied to web services, the RESTful API's are defined with the following aspects:

- Base URI, ex: <http://tpwd.texas.gov/resources/>
- Internet media type for the data, usually JSON (JavaScript object notation) but may include other valid internet media types such as XML, images, etc.
- Standard HTTP methods (GET, PUT, POST, DELETE)
- Hypertext links to reference state
- Hypertext links to reference related resources

RESTful web services may be created in any number of platforms including, but not limited to the following:

- Java through JAX-RS
- C# / .Net
- Python
- Ruby

The web service generally acts as the controller layer for business logic between model (data) and the view (mobile client).

2.8 Sponsorship and Advertising Revenue

Acquire Communications division approval prior to finalizing sponsorship or advertising plans for any external app to ensure consistency and coordination with the agency's sponsorship policy and processes (and with the For-Profit policy in development). Please contact the Marketing group in the Communications division at marketing@tpwd.texas.gov.

2.9 Contracting

When a mobile application will be developed by an external developer for TPWD or for a non-profit partner on behalf of TPWD, TPWD or the non-profit partner will enter into a contract with the developer. At a minimum, the contract should address the following topics:

- Intellectual property ownership

Generally, it is preferable for TPWD or the non-profit partner to own the application and associated intellectual property developed under the contract, especially if TPWD or the non-profit partner is paying the developer to create the application. To ensure this happens, the contract should state that the developer assigns all of its rights in the application, other deliverables, and associated intellectual property developed under the contract to TPWD or the non-profit partner for no additional consideration.

In the event TPWD or the non-profit partner will not own the application or other intellectual property developed under the contract, the contract should clearly state what rights TPWD or the non-profit partner will have. Without ownership rights, it may be difficult for TPWD or the non-profit partner to exercise control over the application.

- Maintenance, updates, and changes

The contract should address the application's anticipated maintenance requirements, including who will perform the maintenance, how often maintenance should be performed and the projected or known costs associated with performing the maintenance. The contract should also address how changes will be made to the application, including updates, bug fixes, corrections, etc.

- Transition plan

The contract should address when and how ownership and/or operational control of the application will be turned over to TPWD or the non-profit partner by the developer. For example, this may occur after a set amount of time, or if a developer goes out of business, or if the developer violates some part of the contract, like not fulfilling its maintenance obligations. The contract should require the developer to work with TPWD or the non-profit partner to ensure all actions required to effectuate the transfer are completed, including transferring the application in iTunes, the Android store, etc.

- Advertising/Sponsorships

The contract should specify whether advertising is allowed and if it is an advertising and/or sponsorship plan will need to be agreed upon and approved by the Communications division. The plan should clearly spell out any restrictions, revenue-sharing arrangements and processes including approvals processes and roles of each party.

- Logo usage

Written approval from Communications division is required for all external facing mobile applications wanting to use the TPWD agency logos or brand(s). For more information, please contact Communications Creative and Interactive Services Group at cis@tpwd.texas.gov.

Applications developed not for the agency but for third parties, such as Friends Groups, cannot carry the Texas Parks & Wildlife brand nor can they be designated as an official app of the agency and instead they must use their own logo.

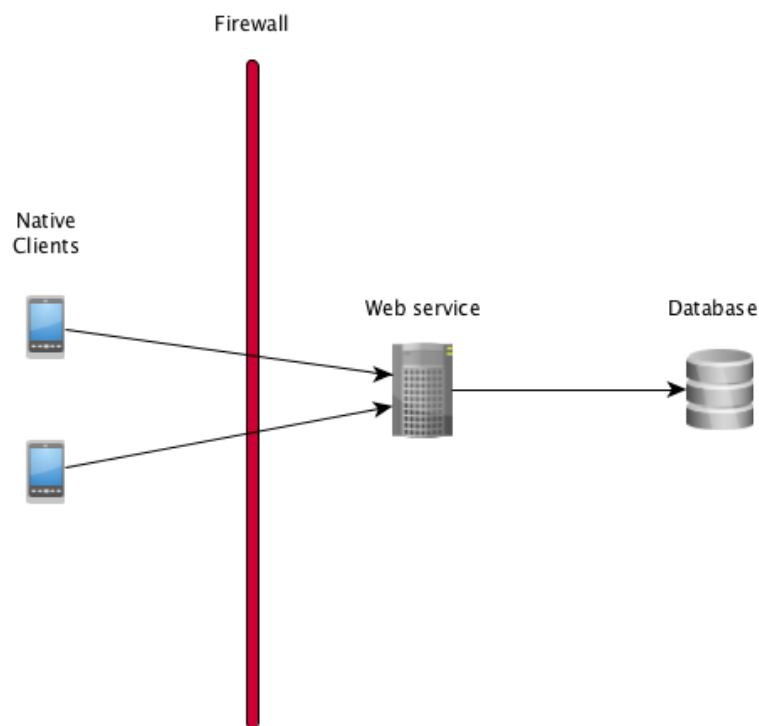
3.0 Mobile Native

3.1 Definition

A native mobile application is one built to run on the device natively such as an iOS application built in Objective C or Swift or an Android application built with Java. It may also include encapsulated mobile web content within a framework that runs natively on the device such as PhoneGap.

Native mobile applications usually run faster than non-native counterparts and have full access to all the features of the device available to it. They may also run without network availability, something that prohibits the use of mobile web pages.

3.2 Architecture



3.3 Platforms

3.3.1 IOS Native

Native iOS applications are created on Apple hardware running OSX along with Xcode. They are usually created using either Objective C or Swift unless a special framework is used, see Multi-Platform Native below.

Apple Developer Program (Licenses)

Two programs exist for Apple iOS development, iOS Developer and iOS Developer Enterprise. iOS Developer allows a company with a development team to create iOS apps for distribution on the App

Store. iOS Developer Enterprise allows a company to create proprietary in-house iOS apps. For TPWD, these apps are distributed through our Sophos mobile device manager.

Anyone wishing to develop native applications will need to be added to the appropriate developer programs and follow any available agency guidelines for iOS development. For further information or to request access to the Apple developer licenses, please send an email to appsupport@tpwd.texas.gov and include 'Developer License' in the subject.

3.3.2 Android Native

Native Android applications are created using Google's Android SDK and generally published through Google Play. There are currently no developer program restrictions. Please contact ITAD for the agency email used to deploy agency Android applications.

3.3.3 Multi – Platform Native

Several cross-platform solutions exist for creating native applications with one code base for multiple device types. These include, but are limited, to the following:

- PhoneGap/Cordova
- Appcelerator
- MoSync
- Xmarin

There is currently no agency recommendation on the use of multi-platform native tools.

3.3.4 Other

Other mobile operating platforms exist such as Windows Mobile, but these are currently beyond the scope of this document.

3.4 Authentication and Security

3.4.1 OAuth

OAuth is an open standard that provides authorization in the form of access tokens. Initially created for use by Twitter, it is designed to work with HTTP and thus fits well with our preferred RESTful web services. The standard allows for expiring tokens for different ids for different applications. Information Technology Application Development currently has a design document detailing the use of OAuth with mobile applications.

4.4.2 Encryption

For confidential data, it is recommended that, in addition to HTTPS, all data be encrypted while in transit from client to server and server to client. At the current writing of this document, it is recommended to use AES 256 or greater encryption.

4.0 Maintenance and Sunset

5.0 Glossary

DIR – Department of Information Resources

Friends Groups – Closely related non-profit partners

TAC – Texas Administrative Code

6.0 Revision History

Version	Date	Name	Description
1.n			
1.0	03/07/2013	Tien Brown	Initial Document

7.0 Appendix

¹ Mobile Methodology:

<http://devjb.tpwd.state.tx.us/mobile-method/#/getting-started/>

² Accessibility and Usability Checklist:

<https://wildnet.tpwd.state.tx.us/insidetrack/divisions/information-technology/application-development/mobile/guidelines/accessibility-checklist/view>

³ Standard Disclaimer:

<https://wildnet.tpwd.state.tx.us/insidetrack/divisions/information-technology/application-development/mobile/guidelines/disclaimer>

IOS Human Interface Guidelines:

https://developer.apple.com/library/ios/documentation/UserExperience/Conceptual/iPhoneAccessibility/Making_Application_Accessible/Making_Application_Accessible.html#//apple_ref/doc/uid/TP40008785-CH102-SW5

Android User Interface Guidelines:

<http://developer.android.com/guide/topics/ui/accessibility/index.html>

TPWD Friends Group Non-Profit Partners:

https://wildnet.tpwd.state.tx.us/ar/partners/partners_friends_groups.phtml

http://www.tpwd.state.tx.us/spdest/friends_groups/

TPWD Security Program: <https://wildnet.tpwd.state.tx.us/insidetrack/divisions/information-technology/technical-services/security/policy-and-standards/itsp/Information-Technology-Security-Program>

State Website Linking and Privacy Policy:

<http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/State%20Website%20Linking%20and%20Privacy%20Policy.pdf>

Creative Services, Publication and Image Standards:

https://wildnet.tpwd.state.tx.us/admin/divisions/communications/creative_services/publication_standards/#usage

Creative Services, TPWD logos:

https://wildnet.tpwd.state.tx.us/admin/divisions/communications/creative_services/logos/index.phtml